



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **05007202 A**(43) Date of publication of application: **14.01.93**

(51) Int. Cl.

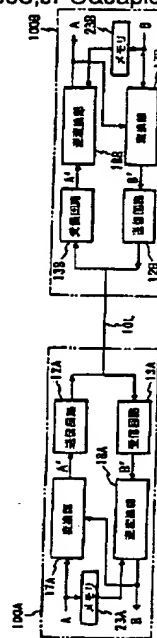
H04L 9/28**H04K 1/04**(21) Application number: **03288717**(22) Date of filing: **05.11.91**(30) Priority: **05.11.90 JP 02299492**(71) Applicant: **NIPPON TELEGR & TELEPH
CORP <NTT>**(72) Inventor: **OKADA KENJI
MANO FUMIO
TOKURA NOBUYUKI
KUMOSAKI KIYOMI
MIKI NORIMOTO****(54) ENCIPHERING COMMUNICATION EQUIPMENT
AND ENCIPHERING TRANSMISSION SYSTEM****(57) Abstract:**

PURPOSE: To realize an enciphering communication device and an enciphering transmission system with high secret.

CONSTITUTION: In an enciphering transmission system where a first communication equipment 100A and a second communication equipment 100B are connected by a transmission line 10L, a first communication equipment 100A has a converting part 17A to encipher an information signal A to be transmitted with a signal corresponding to a receiving signal, and a second communication equipment 100B has an information memory 23B to store information B to be transmitted to the first communication equipment 100A as key information and a reverse converting part 18B to decode an enciphering signal A' received from the first communication equipment 100A with the key information read from the information memory 23B. An enciphering communication equipment 100A has the converting part 17A to encipher a transmitting information signal A with the signal corresponding to the receiving signal, an information memory 23A to store the information signal A to be transmitted as the key information and a reverse converting part 18A to decode a receiving signal B' with

the key information from the information memory 23A. As the transmitting information signal is changed, the key information is changed and the secret is increased.

COPYRIGHT: (C)1993,JPO&Japio



(19)日本国特許庁(JP)

(12)公開特許公報(A)

(11)特許出願公開番号

特開平5-7202

(43)公開日 平成5年(1993)1月14日

(51)Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/28		7117-5K		
H 0 4 K 1/04		7117-5K	H 0 4 L 9/02	A

審査請求 未請求 請求項の数6(全 19 頁)

(21)出願番号 特願平3-288717

(22)出願日 平成3年(1991)11月5日

(31)優先権主張番号 特願平2-299492

(32)優先日 平2(1990)11月5日

(33)優先権主張国 日本(JP)

(71)出願人 000004226

日本電信電話株式会社

東京都千代田区内幸町一丁目1番6号

(72)発明者 岡田 賢治

東京都千代田区内幸町1丁目1番6号 日

本電信電話株式会社内

(72)発明者 真野 文雄

東京都千代田区内幸町1丁目1番6号 日

本電信電話株式会社内

(72)発明者 戸倉 信之

東京都千代田区内幸町1丁目1番6号 日

本電信電話株式会社内

(74)代理人 弁理士 草野 卓

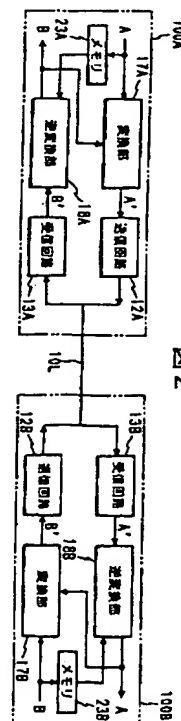
最終頁に続く

(54)【発明の名称】 暗号化通信装置及び暗号化伝送システム

(57)【要約】

【目的】 秘話性の高い暗号化通信装置及び暗号化伝送システムを実現する。

【構成】 第1通信装置100Aと第2通信装置100Bとが伝送路10Lにより接続された暗号化伝送システムにおいて、第1通信装置100Aは受信信号に対応した信号を使って送信すべき情報信号Aを暗号化する変換部17Aを有し、第2通信装置100Bは第1通信装置100Aに送信すべき情報Bをキー情報として記憶する情報メモリ23Bと、情報メモリ23Bから読出したキー情報を使って第1通信装置100Aから受信した暗号化信号A'を復号する逆変換部18Bを有している。暗号化通信装置100Aは受信信号に対応した信号を使って送信情報信号Aを暗号化する変換部17Aと、送信すべき情報信号Aをキー情報として記憶する情報メモリ23Aと、情報メモリ23Aからのキー情報を使って受信信号B'を復号する逆変換部18Aを有している。送信情報信号が変化するとつれキー情報が変化し秘話性の高い暗号化伝送システム及び暗号化通信装置が実現できる。



【特許請求の範囲】

【請求項1】 少なくとも第1と第2の通信装置が伝送媒体を介して接続された暗号化伝送システムにおいて、上記第1通信装置は上記伝送媒体を通して供給された上記第2通信装置からの信号を受信する第1受信手段と、上記第1受信手段から出力される上記第2通信装置からの受信信号に対応した信号を使って上記第2通信装置へ送信すべき情報信号を暗号化して暗号化信号を生成する変換手段と、上記暗号化信号を上記伝送媒体に送出する第1送信手段とを含み、上記第2通信装置は上記第1通信装置に送信すべき情報信号に対応した信号をキー情報として記憶するための情報記憶手段と、上記送信信号を上記伝送媒体に送出する第2送信手段と、上記伝送媒体を通して供給された上記第1通信装置からの上記暗号化信号を受信する第2受信手段と、上記情報記憶手段からの前回送信した上記情報信号に対応する上記キー情報を使って上記第2受信手段で受信された上記暗号化信号を復号して復号化情報信号を出力する逆変換手段とを含む暗号化伝送システム。

【請求項2】 請求項1記載の暗号化伝送システムにおいて、上記第1通信装置の上記変換手段は上記第2通信装置からの受信信号が入力情報として与えられ、それに対応したランダムパターンを生成する第1ランダムパターン生成手段と、上記生成されたランダムパターンと送信すべき上記情報信号との論理演算を行って上記暗号化信号を生成する第1論理演算手段とを含み、上記第2通信装置の上記逆変換手段は上記情報記憶手段からの上記キー情報が入力情報として与えられ、それに対応したランダムパターンを生成する上記第1ランダムパターン生成手段と同じ構成の第2ランダムパターン生成手段と、上記第2ランダムパターン生成手段により生成された上記ランダムパターンと受信された上記暗号化信号とを論理演算を行って上記暗号化信号を復号する第2論理演算手段とを含む。

【請求項3】 請求項1に記載の暗号化伝送システムにおいて、上記第2通信装置と同じ構成の第3通信装置が設けられ、上記伝送媒体は光ファイバ伝送路であり、上記第2及び第3通信装置は方向性光分岐手段により上記光ファイバ伝送路に接続されており、上記第1通信装置内の上記変換手段は上記第2及び第3通信装置に送信すべき送信情報信号をそれぞれ上記第2及び第3通信装置から受信した受信信号を使って暗号化する第1及び第2変換部を含み、上記第1送信手段は上記第1及び第2変換部からの暗号化信号を多重化する多重化手段と、その多重化信号を上記光ファイバ伝送路に送出する光送信回路を含み、上記第1受信手段は上記光ファイバ伝送路から与えられた多重化信号を受信する第1光受信回路と、上記第1光受信回路からの受信多重化信号を上記第2及び第3通信装置からの受信信号に分離する多重分離手段を含み、各上記第2及び第3通信装置内の上記第2受信手段は上記方向性光分岐手段から多重化信号を受信する

第2光受信回路と、上記受信した多重化信号から自分に宛てられた受信信号を分離する分離回路とを含む。

【請求項4】 請求項1記載の暗号化伝送システムにおいて、上記第2通信装置と同じ構成の第3通信装置が設けられ、上記伝送媒体を通じて上記第1通信装置に接続されており、上記第1通信装置の上記第1受信手段は上記伝送媒体を通して上記第2及び第3通信装置から送出され、互いに多重化された多重化信号を受信する第1受信回路と、上記受信多重化信号を上記第2及び第3通信装置からの受信信号に分離する多重分離手段と、上記第2及び第3通信装置へ送信すべき情報信号に対応した信号をキー情報として記憶する第1及び第2情報メモリと、上記多重分離された受信信号をそれぞれ対応した上記第1及び第2情報メモリからの上記キー情報を使って復号化することにより復号化情報信号を出力する第1及び第2逆変換部とを含み、上記第1通信装置の上記変換手段は上記第2及び第3通信装置へ送信すべき情報信号を上記第1及び第2逆変換部からの上記復号化情報信号を使ってそれぞれ暗号化することによりそれぞれ暗号化情報信号を出力する第1及び第2変換部を含み、上記第1送信手段は上記第1及び第2変換部からの上記暗号化情報信号を多重化する多重化手段と、上記多重化された信号を上記伝送媒体に送出する第1送信回路とを含み、上記第2及び第3通信装置のそれぞれにおいて、上記第2受信手段は上記伝送媒体が供給された多重化信号を受信する第2受信回路と、上記第2受信回路からの受信多重化信号から自分に宛てられた受信信号を分離して上記逆変換手段に与える分離回路とを含み、上記第2送信手段は上記逆変換手段からの上記復号化情報信号に対応した信号を使って上記第1通信装置へ送信すべき情報信号を暗号化する変換部と、その暗号化情報信号を上記伝送媒体に送出する第2送信回路を含む。

【請求項5】 伝送媒体を通して供給された信号を受信する受信手段と、上記受信手段からの受信信号に対応した信号の少なくとも一部を使って送信情報信号を論理変換することにより暗号化信号を生成する変換手段と、上記暗号化信号を上記伝送媒体に送出する送信手段と、上記送信情報信号に対応した信号をキー情報として記憶するための情報記憶手段と、上記情報記憶手段からの上記キー情報を使って上記受信手段からの上記受信信号を論理逆変換することにより上記受信信号を復号して復号化情報信号を出力する逆変換手段、とを含む暗号化通信装置。

【請求項6】 請求項5に記載の暗号化通信装置において、上記変換手段は上記受信信号に対応した信号の少なくとも一部を使ってランダムパターンを生成する第1ランダムパターン生成手段と、上記第1ランダムパターン生成手段からのランダムパターンと上記送信情報信号を論理演算して上記暗号化信号を出力する第1論理演算手段を含み、上記逆変換手段は上記情報記憶手段からの上記キー

情報の少なくとも一部を使ってランダムパターンを生成する上記第2ランダムパターン生成手段と、上記第2ランダムパターン生成手段からのランダムパターンと上記受信信号を論理逆変換演算して上記復号化情報信号を出力する第2論理演算手段とを含む。

【発明の詳細な説明】

【0001】

【産業上の利用分野】この発明は複数の暗号化通信装置が伝送路を介して互いに秘話通信を行う暗号化伝送システム及び暗号化通信装置に関する。

【0002】

【従来の技術】従来の秘話通信を行う伝送システムにおいては例えば図1に示すように伝送路10Lに接続された暗号化通信装置100Aと100Bがそれぞれ送信すべき情報を暗号化して相手に送信し、また相手からの暗号化受信信号を解読して情報を得る。各暗号化通信装置はその1つ100Aで説明すると、送信すべき情報信号Aはスクランブル回路11Aにより暗号化され、送信回路12Aにより伝送路10Lに送出される。スクランブル回路11Aは情報信号Aを擬似ランダムパターン発生器15Aにより発生される固定のランダムパターンK1

(暗号化キー)で暗号化する。暗号化された信号A'は送信回路12Aにより伝送路10Lを通して通信装置100Bに送出される。一方通信装置100Bから伝送路10Lを通して受信回路13Aにより受信された信号B'はデスクランブル回路14Aにおいて擬似ランダムパターン発生器16Aにより発生された固定のランダムパターンK2(解読キー)を使って解読され、通信装置100Bからの情報信号Bが得られる。

【0003】

【発明が解決しようとする課題】図1のような従来の暗号化伝送システムにおいては、秘話性を高めるため暗号化のために使用するランダムパターンK1、K2として非常に長いランダムパターンを使用し、かつ複雑な変換を行おうとすると、スクランブル回路11A、11B、及びデスクランブル回路14A、14Bの回路規模が大きくなり、価格が高くなる欠点がある。しかも使用するランダムパターンK1、K2は固定されているため、第三者に解読される可能性を皆無に近かづけることは困難である。例えば同様の構成の暗号化通信装置が100A、100B以外にも伝送路10Lに接続されている場合に、それぞれの通信装置のスクランブル回路及びデスクランブル回路を同様な仕様の回路で構成し、同様の交換規則や交換周期を適用すると通信装置間の秘話性を低くめてしまう。

【0004】この発明の目的は構成が簡単でかつ秘話性の高い暗号化通信装置を提供することである。この発明のもう1つの目的は構成が簡単でかつ秘話性の高い暗号化伝送システムを提供することである。

【0005】

【課題を解決するための手段】この発明による暗号化通信装置は受信された信号を用いて送信信号を論理変換し、それによって暗号化信号を生成する変換手段と、その暗号化信号を伝送路に送出する送信回路手段と、上記送信信号に対応した信号をキー情報として記憶する情報記憶手段と、上記伝送路から与えられる暗号化信号を受信する受信回路手段と、上記情報記憶手段からの上記キー情報を使って上記受信暗号化信号を論理逆変換することにより解読した受信信号を出力する逆変換手段とを含む。

【0006】この発明による暗号化伝送システムは少なくとも第1と第2の通信装置が伝送路を介して接続され、上記第1通信装置は上記第2通信装置からの信号を受信する第1受信回路手段と、その受信信号を使って送信信号を論理変換し、それによって暗号化信号を生成する変換手段と、その暗号化信号を上記伝送路に送出する第1送信回路手段とを含み、上記第2通信装置は送信すべき信号をキー情報として記憶する情報記憶手段と、上記送信すべき信号を上記伝送路に送出する第2送信回路手段と、上記伝送路から与えられる暗号化信号を受信する第2受信回路手段と、上記情報記憶手段からの上記キー情報を使って上記受信した暗号化信号を論理逆変換することにより解読した信号を出力する逆変換手段とを含む。

【0007】

【作用】この発明の暗号化通信装置及び暗号化伝送システムによれば通信相手からの順次変化する受信信号を使って送信信号を暗号化しているので、通信相手以外の者が暗号化された送信信号を解読することは非常に困難である。また受信信号を使った送信信号の暗号化は比較的簡単な論理変換によっても高い秘話性を実現することが可能である。従って各通信装置の回路規模を比較的小さく、安価に製造することができる。

【0008】図2はこの発明を適用した2つの暗号化通信装置100A、100Bが伝送路10Lに接続された暗号化伝送システムの実施例を示している。伝送路10Lに接続される暗号化通信装置は2つ以上でもよく、それぞれ同様の構成とされているので代表して通信装置100Aを以下に説明する。暗号化通信装置100Aは送信回路12Aと、受信回路13Aと、変換部17Aと逆変換部18Aと、送信情報メモリ23Aとによって構成されている。変換部17Aは受信情報信号Bと送信情報信号Aとの排他的論理和をとる排他的論理和回路や、その他の論理演算回路のような簡単なものでよく、逆変換部18Aも同様である。あらかじめ決めた長さの送信すべき情報信号Aは変換部17Aに与えられ、逆変換部18Aからの最新の復号情報信号Bを使って論理変換により暗号化されると共にキー情報として情報メモリ23Aに与えられ、次の受信暗号化情報信号B'の復号化まで記憶される。暗号化された信号A'は送信回路12Aに

より伝送路10Lを通して相手暗号化通信装置100Bに送出される。

【0009】その後伝送路10Lを通して相手暗号化装置100Bから受信回路13Aに供給された受信暗号化信号B'は逆変換部18Aにおいて情報メモリ23Aから読出したキー情報信号Aを使って論理逆変換により解読(復号)され、情報信号Bが得られる。一方、次に送信すべき情報信号Aが新しいキー情報として情報メモリ23Aに与えられて内容が書き換えられ、またその情報信号Aが変換部17Aに与えられる。復号された情報信号Bはこの送信すべき情報信号Aの暗号化のために変換部17Aに与えられる。このようにして情報信号Bを使って暗号化された信号A'は暗号化通信装置100Bにおいて情報メモリ23Bに記憶してあるキー情報信号Bを使って復号することが可能であり、また暗号化通信装置100Bにおいて復号された情報信号Aを使って暗号化された信号B'は暗号化通信装置100Aにおいて情報メモリ23Aに記憶してある情報信号Aを使って復号することが可能である。しかしながら情報信号A、Bは随時変化していくので情報信号A及びBのいずれも得ていない通信装置においては暗号化信号A'及びB'を解読することは困難である。

【0010】図2の実施例の動作例を図3の表Iを参照して説明する。ただし簡単のため各情報信号A、Bは8ビット長であり、変換部17A、17B及び変換部18A、18Bはすべて排他的論理和回路で構成するものとする。また初期状態として情報メモリ23A、23Bの内容はすべて“0”であり、逆変換部18Aの出力Bの初期値B₀はオール“0”であるとする。暗号化通信装置100Aは情報信号A₁、A₂、…を順次送信するものとし、暗号化通信装置100Bは情報信号B₁、B₂、…を順次送信するものとする。更に、図3中に使用されている排他的論理和を表す一般的な記号である丸十字は以下の説明文において記号*で表す。

【0011】まず暗号化通信装置100Aにおいては情報信号A₁:10101010をキー情報としてメモリ23Aに格納すると共に変換部17Aに与え受信情報信号初期値B₀:00000000との排他的論理和A₁*B₀=A₁'を1ビットずつ演算し、その結果A₁':10101010を相手通信装置100Bに送信する。通信装置100Bでは逆変換部18Bによりメモリ23B内のキー情報の初期値B₀:00000000と受信信号A₁'との排他的論理和A₁'*B₀=A₁を1ビットずつ演算して受信情報信号A₁:10101010を得る。更に送信すべき情報信号B₁:00001111を新しいキー情報としてメモリ23Bに書き込むと共に変換部17Bにより受信情報信号A₁との排他的論理和A₁*B₁=B₁'を1ビットずつ演算し、その結果B₁':10100101を送信する。通信装置100Aは受信信号B₁'とメモリ23Aの内容A₁と

の排他的論理和A₁*B₁'=B₁を逆変換部18Aで演算してB₁=00001111を得る。更に次に送信すべき情報信号A₂:00110011でメモリ23Aを書き換えると共に変換部17AでA₂*B₁=A₂'を演算し、その結果A₂'=00111100を送信する。通信装置100Bにおいてはメモリ23Bの内容B₁と受信信号A₂'とから、A₂'*B₁=A₂を逆変換部18Bで演算して情報信号A₂=00110011を得る。更に次に送信すべき情報B₂=11100010でメモリ23Bを書き換えると共に変換部17BによりA₂*B₂=B₂'を演算してその結果B₂'=11010001を送信する。通信装置100Aではメモリ23Aの内容A₂と受信信号B₂'からA₂*B₂'=B₂を逆変換部18Aにより演算し、以下同様な手順が繰り返される。

【0012】ところで上述の例のように変換部17Aを単純な排他的論理和回路のみで構成した場合、図3を参照して説明したように通信の開始時に受信情報信号Bの初期値B₀がオール“0”であると、最初の送信情報信号A₁は排他的論理和回路による変換後も同じ信号即ちA₁'=A₁となってしまう第3者に対し、解読のための手掛かりを与えてしまう。同様に通信中における送信情報信号Aがたまたまオール“0”となるとその時受信した情報信号Bがそのまま変換部17Aから出力されてしまい第3者に対し解読の手掛かりを与えてしまう。

【0013】情報信号A及び/又はBがオール“1”の場合も同様である。このような生の情報の流出を避けるには第1図と同様に第4図に示すように送信情報信号Aをスクランブル回路11Aにおいて擬似ランダムパターン発生器15Aからの固定ランダムパターンK₁により論理変換してから図2における同様の送信処理を行い、逆変換部18Aから出力された受信情報信号はデスクランブル回路14Aにおいて擬似ランダムパターン発生器16Aからの固定ランダムパターンK₂により論理逆変換すればよい。スクランブル回路11A及びデスクランブル回路14Aとしては例えば排他的論理和回路や他の論理演算回路を使用することができる。

【0014】なお、スクランブル回路11Aは本来送信情報信号Aをランダム化(交流化)するためのものであり、それ自体は暗号化を目的とするものではない。従って、キー情報の初期値をオール“0”及びオール“1”以外のあらかじめ決めた値に設定し、しかも送信情報信号Aが“0”の連続または“1”の連続とならない保証があれば、スクランブル処理を行わないでもよい。逆に、スクランブル処理を行うことにより秘話性を高めることが可能となる。更に通信装置100Aと相手通信装置(図示せず)とが使用するスクランブルパターン(擬似ランダムパターン)K₁とK₂が同じ長さでも異なるパターンとなるように選べばそれだけ秘話性は高くなり、更に長さ(ビット数)を異ならせれば一層秘話性が向上す

る。また上述の例では例えば暗号化通信装置100Aのスクランブル回路11Aにおける情報信号Aに対する擬似ランダムパターンK1の位相と暗号化通信装置100Bのデスクランブル回路14Aにおける受信暗号化信号A'に対する擬似ランダムパターンK1の位相を同期させる、いわゆる外部同期方式を用いる必要があるが、このような外部からの固定の擬似ランダムパターンを与えないで、ビット毎に入力される情報信号を例えば排他的論理和回路の一方の入力端子に供給し、その排他的論理和回路の出力をあらかじめ決められた段数のシフトレジスタを通して排他的論理和回路の他方の入力端子に帰還し、排他的論理和回路の出力をスクランブル回路の出力とするような公知の自己同期形スクランブル回路を使用してもよい。このような自己同期形スクランブル回路に対する自己同期形デスクランブル回路もよく知られている。

【0015】図2及び図4の実施例において更に秘話性を高めるため変換部17Aをランダムパターン生成回路と論理変換回路により構成してもよい。その場合の暗号化通信装置100Aの例を図5に示す。変換部17Aのランダムパターン生成回路21Aは復号情報信号Bの全ビットまたはそのあらかじめ決めた複数のビットに対応したランダムパターンを生成出力する。論理変換回路22Aは前述のような排他的論理和回路やその他の論理演算回路でよい。逆変換部18Aも同様にランダムパターン生成回路24Aと論理逆変換回路25Aにより構成してもよい。このように復号情報信号Bにより直接送信情報信号Aを変換することとを避けることにより、例えば通信の開始時や通信中において情報信号A及び／又はBがたまたまオール“0”またはオール“1”となっても高い秘話性を維持することが可能である。しかも情報信号A、Bは順次変化していくので、生成されるランダムパターンも順次変化し、高い秘話性を実現できる。

【0016】逆変換部18Aのランダムパターン生成回路24Aは変換部17Aのランダムパターン生成回路21Aと全く同じ構成である必要はない。暗号化通信装置100Bについても同様であるが変換部17Bと逆変換部18Bのランダムパターン生成回路(図示せず)はそれぞれ暗号化通信装置100Aにおける逆変換部18Aと変換部17Aのランダムパターン生成回路24A及び21Aと全く同じ構成である必要がある。

【0017】図6は図5におけるランダムパターン生成回路21A、24A(変換部17B、逆変換部18Bに用いられる場合も同様)の一実施例を示し、割算回路31と非線形演算回路32により構成されている。割算回路31は与えられた情報信号AまたはB、またはその一部をあらかじめ決めた生成多項式で割算し、その剰余を非線形演算回路32に与える(例えばW. W. Peterson and E. J. Weldon "Errorcorrecting codes," M. I. T. Press, 1972)。非線形演算回路32はその出力から入力を推定することが困難な非可逆的演算を行う回路であり、

その演算結果はランダムパターンとして出力される。このような非線形演算回路32を2次のリカーブフィルタで構成した例を図7に示す。

【0018】この非線形演算回路32は演算回路31から与えられた剰余に対応した初期値が設定され、その初期値からランダムパターンを発生するものであり、図7に示すように例えば2段の並列8ビットシフトレジスタ

(即ち2段の遅延回路)を構成する8ビットD形フリップフロップ回路41、42と、ビットシフト43と、8ビット加算器44とから構成される。各8ビットD形フリップフロップ回路41、42にそれぞれ設定する8ビットの初期値としては割算回路31から与えられた剰余のあらかじめ決めた8ビットの同じデータを用いてもよいが、図7の実施例ではその8ビットデータをフリップフロップ回路41に設定すると共に、論理反転回路54で前記8ビットデータの全8ビットの論理を反転してフリップフロップ回路42に設定する。

【0019】フリップフロップ回路41に設定された8ビットデータはビットシフト43で全ビットが例えば下位方向に所定ビット数、例えば1ビットシフトされ(即ち8ビットデータが2で割算され)、アンダーフローが捨てられると共にその8ビット出力が8ビット加算器44の一方の入力に与えられる。加算器44の他方の入力にはフリップフロップ回路42の8ビットの内容が与えられる。加算により生じたオーバフローは捨てられ、8ビットの加算結果がランダムパターンシーケンス中の部分パターンとして出力されると共にフリップフロップ回路41のデータ端子D(8ビット)に与えられている。この状態でフリップフロップ回路41、42のクロック端子CKにクロック信号CKが与えられると、フリップフロップ回路41の8ビットQ出力がフリップフロップ回路42に取り込まれると共に、フリップフロップ回路41に、そのデータ端子Dに与えられていたデータが取り込まれ、その結果次の部分パターン(8ビット)が加算器44から出力される。

【0020】クロック信号CKは情報信号AまたはBの8ビット毎にフリップフロップ回路41、42に与えられ、例えば情報信号A、Bの長さが128バイトであればクロック信号CKを128回与えてからフリップフロップ回路41、42をリセット信号Rによりリセットし、次の情報信号A、Bにもとづいて新しい初期値を再びフリップフロップ回路41、42にプリセットし、同様の動作を繰り返す。なお、ビットシフト43は入力8ビットデータを上位方向に所定ビット数シフト(即ち2の巾乗の乗算)して、オーバフローを捨ててもよい。このように加算器44のオーバフローや割算器(または乗算器)43のアンダフロー(またはオーバフロー)を捨てることにより演算の非可逆性を実現することができる。

【0021】このように簡単な割算回路31と2次のリ

カーシブフィルタ32により構成された図6のランダムボタン生成回路21Aにより、入力情報信号A、Bに従って一義的に定まるランダムボタンを部分ボタン毎に順次生成することができ、かつこれら一連の部分ボタンから情報信号A、Bを推定することは非常に困難である。リカーシブフィルタ32の次数を高くすれば更に秘話性を高めることができることは明らかである。

【0022】図8はランダムボタン生成回路21A、24A（通信装置100Bにも同様に設けられる）の更に他の実施例を示し、論理演算回路33と、識別番号メモリ34と、デコーダ35と、固定ボタンメモリ36と、切替スイッチ37とにより構成されている。識別番号メモリ34には、その暗号化通信装置にあらかじめ割り当てられた識別番号IDが記憶されている。論理演算回路33は与えられた情報信号A（またはB）と識別番号メモリ34からの識別番号IDまたはそのあらかじめ決めた一部とを論理演算してその結果をランダムボタンとして切替スイッチ37を介して出力する。デコーダ35は入力情報信号A（またはB）がオール“0”及びオール“1”であることを検出すると制御信号を出力して切替スイッチ37を固定ボタンメモリ36側に接続し、固定ボタンメモリ36に保持してあるオール“0”及びオール“1”以外のあらかじめ決めた1つの固定ボタンを出力する。このように構成することによりランダムボタン生成回路21A、24Aに与えられる情報信号A（またはB）がオール“0”またはオール“1”の場合に識別番号メモリ34に保持している装置識別番号がそのまま変換回路22A、または逆変換回路25Aに与えられることを防ぐことができる。なお、切替スイッチ37は論理演算回路33の出力側ではなく、論理変換回路22A（論理逆変換回路25A）の出力側に挿入してもよい。

【0023】図9はランダムボタン生成回路21A、24Aの更に他の実施例を示す。この実施例は複数、例えば8個の異なるランダムボタンから入力情報信号A（またはB）に応じてそのうちの1つを選択して出力するものであり、以下のように構成される。タイマ回路51は受信回路13Aで再生したクロック信号CKとフレーム同期信号FSYNが与えられ、後者によりリセットされ、前者を計数し、計数値が所定値に達するとタイムアップ信号TUを出力し、セクタ53のロード端子Lに与える。フレーム同期信号FSYNはタイマ回路51を通して8進カウンタのリセット端子Rにも与えられる。8進カウンタ52は情報信号A（またはB）が与えられ、その一連のビット中の“1”（または“0”）を順次計数する。タイマ回路51がタイムアップ信号TUをセクタ53のロード端子Lに与えると、セクタ53はその時の8進カウンタ52の計数値を取り込み、その計数値に従ってランダムボタン発生器R1～R8の1つを選択し、そこから発生されるランダムボタンを出力する。各ランダムボタン発生器R1～R8としては、例え

ばシフトレジスタと排他的論理和回路により構成された周知の擬似ランダムボタン発生回路でもよいし、必要な数（ここでは8個）のランダムボタンを記憶したROMでもよいし、あるいはランダムボタン発生手順をプログラム化したソフトであってもよい。

【0024】以上いくつかの例で説明したランダムボタン生成回路を用いた暗号化通信装置において、生成したランダムボタンからの入力情報信号の解読を更に困難にするように構成した暗号化通信装置100Aの実施例を図10に示す。図2における暗号化通信装置100Aとの相異点は変換部17A及び逆変換部18Aにおいてランダムボタン生成回路21A及び24Aの入力側にボタン縮退回路26A及び27Aをそれぞれ挿入した点である。ボタン縮退回路26A、27Aは 2^n 個の可能な異なる入力ボタン（nビット）のそれぞれに対し 2^n より少ないM個の異なるボタンのあらかじめ決めたいずれか1つを割り当てて出力するものであり、従って複数の異なる入力ボタンに対し同一の出力ボタンが出力される。例えば異なる2つの決められたボタンの受信情報信号Bに対しボタン縮退回路26Aが同一のボタンを出力すると、ランダムボタン生成回路21Aも同一のランダムボタンを出力する。ランダムボタン生成回路21Aから出力されたそのランダムボタンから受信情報信号Bが前記2つのボタンのいずれであったか判定することはできない。なお図10の実施例においてランダムボタン生成回路21Aとボタン縮退回路26Aの位置を入れ替えてもよく、ランダムボタン生成回路24Aとボタン縮退回路27Aの位置を入れ替えてもよい。

【0025】図11は図10の実施例におけるボタン縮退回路26A、27Aの一実施例を示す。このボタン縮退回路は2段シフトレジスタ46と、AND回路47と2段のシフトレジスタ48とから構成されている。情報信号AまたはBの2ビットが、シフトレジスタ46にシリアルにロードされる毎にシフトレジスタ46の2つの段の出力Q1、Q2が入力端子X1、X2を介してAND回路47の入力端子に与えられ、それらの論理積が出力端子Y1に出力される。一方出力Q2は入力端子X2を介して出力端子Y2に出力される。これら出力端子Y1、Y2からの出力はシフトレジスタ48の2つの段に並列入力され、その後シフトレジスタ47からシリアルに出力されると共に情報信号A（またはB）の次の2ビットがシリアルにシフトレジスタ45に入力され同様の動作が繰り返される。この結果、端子X1、X2に与えられる2ビットボタンと出力端子Y1、Y2に得られる2ビットボタンの関係は図12の表IIに示ようになる。即ち入力ビットボタンが“00”及び“10”の場合、いずれも出力ビットボタンは“00”となる。従ってこのボタン縮退回路の出力ボタンから入力ボタンを推定できる確率はそれだけ低くなる。

【0026】図13は図2の実施例における各暗号化通

信装置の他の実施例を通信装置100Aで代表して示す。この実施例では受信回路13Aの出力である受信された暗号化信号B'中の符号誤りを検出する誤り検出回路28Aが設けられている。またランダムパターン生成回路21A、24Aにより生成されたランダムパターンはボタンメモリ38A、39Aに取り込まれ、そこから変換回路22A及び逆変換回路25Aに与えられる。誤り検出回路28Aは例えばよく知られているCRC誤り検出方法を用いたものであり、受信暗号化信号B'中の符号誤りを検出すると検出信号Eaをボタンメモリ38Aのインヒビット端子INHに与えると共に送信回路12Aにも与える。ボタンメモリ38Aは検出信号Eaによりランダムパターン生成回路21Aからのランダムパタンの取り込みが禁止され、従ってそれまで保持していたランダムパターンは更新されず、再び論理変換回路22Aに供給される。論理変換回路22Aはそのランダムパターンにより情報信号Aを暗号化し、送信回路12Aはその暗号化情報信号A'の先頭に誤り検出信号Eaを付加して伝送路10Lに送出する。誤り検出回路28Aが誤り検出信号Ea(1ビット)を出力している限りこの動作は繰り返され、誤り検出信号Eaが出力されなくなるとボタンメモリ38Aはランダムパターン生成回路21Aからのランダムパタンの取り込みを再開する。

【0027】一方、相手通信装置100Bが受信暗号化信号A'中に符号誤りを検出した場合、上記と同様の動作を行い、その結果、暗号化情報信号B'に誤り検出信号Ebが付加されて通信装置100Aに送信される。通信装置100Aの受信回路13Aは受信暗号化信号B'中に誤り検出信号Ebが付加されているのを検出するとその信号Ebにより逆変換部18Aのボタンメモリ39Aの取込み動作を禁止する。従ってそれまでボタンメモリ39Aに保持されていたランダムパターンを使って逆変換回路25Aにより受信暗号化信号B'の復号が行われる。このようにして受信信号B'中に符号誤りが検出された場合には、その誤りを含む受信情報信号Bにもとづいてランダムパターン生成回路21Aで発生されるランダムパターンを使用しないで、その直前に生成したランダムパターンを使って情報信号Aの暗号化を行うと共に、相手通信装置100Bに誤り検出信号Eaの送信するので、正しい復号化及び暗号化処理を継続することができる。なお、誤り検出信号Ea、Eb自体の伝送路上での符号誤りの影響を回避するため、例えば誤り検出信号Ea、Ebを複数回送信し、受信側において多数決により、誤り信号を判別してもよい。

【0028】上述した図5、図10及び図13の各実施例では情報信号Aを暗号化するためのランダムパターンは復号化後の情報信号Bを使ってランダムパターン生成回路21Aにより生成し、また暗号化受信信号B'を復号するためのランダムパターンは暗号化前の情報信号Aを使ってランダムパターン生成回路24Aにより生成する場合を

示したが、逆に復号化前の受信信号B'を使って情報信号Aを暗号化するためのランダムパターンを生成し、暗号化された情報信号A'を使って受信信号B'を復号するためのランダムパターンを生成してもよい。その場合の暗号化通信装置100Aの例を図5と対応させて図14に示す。その通信装置100Aの動作原理は図5の場合と同様なので説明を省略する。

【0029】以上説明したこの発明の暗号化通信装置及び暗号化伝送システムは1対1の暗号化通信の場合であったが、この発明はそれに限定されるものでなく、1対複数(ポイント-マルチポイント)の伝送システムにも適用できることは明かである。その例を図15に示す。この伝送システムにおいては通信装置100Aは伝送路10Lを通して複数、例えば2つの通信装置100B、100Cと多重通信を行う。多重化方法は時分割多重、周波数多重、あるいはその他の多重化方法を使ってよい。ここで通信装置100Aをセンタ装置と呼び、通信装置100B、100Cを加入者装置と呼ぶことにする。センタ装置100Aは加入者装置100B、100Cに対しそれぞれ送信すべき情報信号A1、A2を変換部17A1、17A2により加入者装置100B、100Cからの復号情報B、Cを使ってそれぞれ暗号化する。この時これまでの実施例の場合と同様に情報信号A1、A2は情報メモリ23A1、23A2にキー情報としてそれぞれ保持される。暗号化情報信号A1'、A2'は多重化回路54で多重化され、送信回路12Aにより伝送路10Lに送出される。

【0030】加入者装置100Bは受信回路13Bにより受信したセンタ装置100Aからの多重化信号から分離回路55Bにより自分宛の暗号化情報信号A1'を分離し、逆変換部18Bにおいて情報メモリ23Bに保持してあるキー情報、即ち前回に送信した情報信号Bを使って復号して情報信号A1を得る。加入者装置100Bは更に次に送信する情報信号Bを情報メモリ32Bに格納すると共にこの復号情報信号A1を使って変換部17Bにより暗号化し、その暗号化情報信号B'を送信回路12Bにより伝送路10Lに送出する。ただし、この伝送システムがTDMAのような同期形時分割多重方式を利用している場合は信号B'の送出は加入者装置100Bに割当てられたタイムスロットを使って行われ、非同期形の時分割多重を利用している場合はアドレスが付加されたバケットを使って行われ、周波数多重を利用している場合は割当てられた周波数を使って行われる。加入者装置100Cも同様の動作により復号情報信号A2を得ると共に情報信号Cを送信する。センタ装置100Aは受信回路13Aにより受信した多重化信号を分離回路55Aにより分離して加入者装置100B、100Cからの暗号化情報信号B'、C'を得て、それらをそれぞれ逆変換部18A1、18A2によりそれぞれ情報メモリ23A1、23A2に保持してあるキー情報A1、A

2を使って復号し、情報信号B、Cを得る。

【0031】図15の暗号化伝送システムにおける各通信装置100A、100B、100Cの変換部17A1、17A2、17B、17C、逆変換部18A1、18A2、18B、18Cに前述した図6、8及び9やその他各種のランダムパタン生成回路を適用できることはいうまでもない。また各通信装置100A、100B、100Cにおいて図4に示すようにスクランブル回路11A、デスクランブル回路14A、擬似ランダムパタン発生器15A、16Aを設け、各装置の送信側においては送信情報信号を固定擬似ランダムパタンで暗号化してから変換部により受信信号にもとづいて暗号化し、受信側においては受信信号を逆変換部で復号してからデスクランブル回路14Aで固定擬似ランダムパタンにより最終的に復号するようにしてもよい。また図10に示すようにパタン縮退回路26A、27Aにより情報信号をその複数の異なる部分パタンが同一の部分パタンとなるようにパタン変換してから、それにもとづいてランダムパタンを発生してもよい。更に図13を参照して説明したように誤り検出回路28Aを設け、かつ変換部及び逆変換部のランダムパタン生成回路で生成されたランダムパタンをパタンメモリ38A、39Aに格納してから変換回路及び逆変換回路に与えるようにし、受信信号中に符号誤りを検出した場合はその検出信号を相手通信装置に送信すると共にパタンメモリへのランダムパタンの書き込みを禁止するよう構成してもよい。また図2及び図15に示したこの発明の暗号化伝送システムでは伝送路10Lは電気信号ケーブルに限定されず、電波の空間伝播路であってもよく、光ファイバ伝送路であってもよい。

【0032】図15のポイント-マルチポイント伝送システムに光ファイバ伝送方式を適用した場合の実施例を図16に示す。センタ装置100Aからの共通の光ファイバ伝送路10Lに複数の加入者装置100B、100Cからの個別光ファイバ線路La、Lbが方向性光分岐器57によりそれぞれ接続されており、センタ装置100Aが送出する多重化信号は図15の場合と同様に同報的にすべての加入者装置100B、100Cに送信される。図15の場合と同様に各加入者装置においては自分以外の加入者装置に送信された信号を容易に分離して取り出すことができ、従ってセンタ装置100Aから各加入者装置100B、100Cへ送信される信号は暗号化されている必要がある。しかしながら各加入者装置は方向性光分岐器57で光ファイバ伝送路10Lに接続されているので、各加入者装置から送信される送信信号は他のいずれの加入者装置にも洩れることなく、センタ装置100Aにのみ送信することができる。従って図16の実施例においては加入者装置100B、100Cから送出する信号は暗号化しないで送出している。センタ装置100Aは図15における逆変換部18A1、18A2、情報メモリ23A1、23A2を有しておらず、光

受信回路13Aで受信した多重化信号を分離回路55Aにより各加入者装置100B、100Cからの情報信号B、Cに分離し、その情報信号B、Cを使って変換部17A1、17A2において送信すべき情報信号A1、A2を暗号化する。暗号化情報信号A1'、A2'は多重化回路54により多重化され、光送信回路12Aにより光カプラ56Aを通して光ファイバ伝送路10Lに送出される。送信信号は方向性光分岐器57により分岐され全ての加入者装置100B、100Cに供給される。各加入者装置100B、100Cは図15における変換部17B、17Cを有しておらず、装置100Bで代表して説明するように光受信回路13Bにより受信した多重化信号から分離回路55Bにより自分宛の暗号化信号A1'を分離し、逆変換部18Bにおいて情報メモリ23Bに保持してあるキー情報、即ち前回の送信情報信号Bを使って受信暗号化信号A1'を復号し、情報信号A1を得る。加入者装置100Bが送信すべき情報信号Bは暗号化せずそのまま光送信回路12Bにより光カプラ56B、及び方向性光分岐器57を通して光ファイバ伝送路10Lに送出される。

【0033】図16の実施例においても各変換部17A1、17A2と逆変換部18B、18Cを単純な排他的論理和回路で実現してよいし、更に秘話性を高めるため図5の場合のように各変換部17A1、17A2をランダムパタン生成回路21Aと論理変換回路22Aにより構成し、各逆変換部18B、18Cをランダムパタン生成回路24Aと論理逆変換回路25Aとにより構成してもよい。その場合、各ランダムパタン生成回路として前述したような各種の実施例を適用することができる。なお、センタ装置100Aは通常伝送システム全体を制御する機能を持たされており、また各加入者装置が図6または図8のランダムパタン生成回路に使用する生成多項式または識別番号IDを全て持っている。

【0034】更に図4の実施例のようにセンタ装置100Aにおいては変換部17A1、17A2の入力側とスクランブル回路を設けて送信すべき情報信号A1、A2をあらかじめ固定パタンで暗号化すると共に分離回路55Aにより分離された受信情報信号をデスクランブル回路により復号して情報信号B、Cを得るようにしてもよい。この場合、各加入者装置100B、100Cにおいても逆変換部18B、18Cの出力側にデスクランブル回路を設け、また送信情報信号の入力側にスクランブル回路を設け、送信すべき情報信号B、Cをあらかじめスクランブル回路により暗号化してから送信処理を行うように構成する。

【0035】更に図16の実施例に図10で説明したパタン縮退回路26A、27Aの使用を適用してもよい。また図13の実施例を図16に適用することもできる。即ちセンタ装置100Aの各変換部17A1、17A2を図13に示す変換部17Aと同じ構成とし、分離回路

55Aの各分離出力側に誤り検出回路をそれぞれ接続する。各誤り検出回路の誤り検出力は対応する変換部のパタンメモリにインヒビット信号として与えると共に多重化回路54に与え、暗号化情報信号A1'、A2'の多重化の際に対応する暗号化情報信号の例えば先頭に誤り検出信号を表す符号(1ビット)を付加する。各加入者装置100B、100Cにおいては逆変換部18B、18Cを図13の逆変換部18Aと同じ構成とし、分離回路55B、55Cの出力にそれぞれ誤り検出符号検出器を接続し、その検出力を逆変換部18B、18Cのパタンメモリにインヒビット信号として与える。

【0036】次に図16の実施例においてセンタ装置100Aと加入者装置100B、100C間の信号の伝送方式を表すタイムチャートの例をいくつか示す。なお図が繁雑となるので暗号化後の情報信号は上述で使ったダッシュを付けずに暗号化前の情報信号と同じ記号で表す。また、破線矢印Enは暗号化処理を表し、破線矢印Deは復号処理を表す。

【0037】図17は加入者装置100B、100Cからセンタ装置100Aへの上り信号とその逆の下り信号をTDMAのように送受信のタイミングが同期した時分割多重する場合のタイムチャートを示し、信号送受信周期(即ち繰返し周期)T_fが一定の場合である。センタ装置100Aから加入者装置100B、100C宛の暗号化信号A1₁、A2₁(一定長)があらかじめそれぞれの加入者装置に割り当てられたタイムスロットで送信され、加入者装置100B、100Cはそれぞれ自分に割り当てられたタイムスロットから暗号化信号A1₁、A2₁を抽出し、前回の送信情報(図示せず)を使って復号し、一定時間T_x後に情報信号B₁、C₁を送出する。センタ装置100Aは情報信号B₁、C₁を受信し、その情報信号を使って次に送信する情報A1₂、A2₂を暗号化し、前回の送信から時間T_f後に所定のタイムスロットで送信する。加入者装置100B、100Cはそれぞれ受信した暗号化情報A1₂、A2₂をそれぞれ前回の送信情報信号B₁、C₁を使って復号し、一定時間T_x後に情報信号B₂、C₂をそれぞれ送信する。以下同様の動作が繰り返される。

【0038】図18は送受信のタイミングが非同期で時分割多重を行う方式の信号送受タイムチャートを示す。センタ装置100Aは各加入者装置から受けた最新の復号受信情報を少なくとも次の復号受信信号が得られるまで保持する機能を有しており、各加入者装置100B、100Cに対しそれらのアドレスが先頭に付加された暗号化情報信号をパケットとして任意のタイミングで送信する。各加入者装置100B、100Cは送信すべき情報信号B、Cの先頭に自分のアドレスを付加したパケットを任意のタイミングで送信する。ただし、センタ装置100Aも、加入者装置100B、100Cもすべて信号衝突検出機能を有し、信号送出中に信号衝突を検出し

た場合はそのパケットの送信をやりなおす。

【0039】図19は上り信号と下り信号を別々の光ファイバ線路、または異なる波長で伝送する場合の伝送方式の一例を示すタイムチャートである。この伝送方式の例においては、センタ装置100Aは各加入者装置宛の送信信号A1₁、A2₂、…、A2₁、A2₂、…をあらかじめ各加入者装置に割り当てたタイムスロットに時分割多重して連続して送信すると同時に、加入者装置100B、100Cからの送信信号B₁、B₂、…及びC₁、C₂、…も時分割多重されて連続して受信することができる特徴がある。

【0040】図17～19のいずれの伝送方式においても、センタ装置100Aと各加入者装置100B、100C間の通信において上り信号と下り信号の伝送容量が不平衡の場合は、例えば変換部において送信情報信号を暗号化するのに使用する受信情報信号はその一部を使用するか、あるいは一連の送信情報信号に対し同一の受信情報信号を複数回使用するようにすればよい。

【0041】以上説明したように、この発明による暗号化通信装置によれば、復号受信信号または受信暗号化信号を使って変換部により送信すべき情報信号を暗号化して送出すると共に、送信情報信号または暗号化情報信号をキー情報として情報メモリに相手装置からの応答情報信号の受信時まで記憶しておき、情報メモリから読み出された前回の情報信号送信時のキー情報を使って逆変換部において暗号化受信信号を復号するように構成されている。暗号化及び復号化に使用する情報は随時変化するので秘話性の高い通信が可能な暗号化通信装置を実現することができる。更に、伝送路を通して少なくとも2つの通信装置が接続されたこの発明の暗号化伝送システムによれば、第1の通信装置においては受信信号を使って送信すべき情報信号を変換部において暗号化して第2の通信装置へ送出し、第2通信装置においては情報メモリに保持されている前回の情報信号であるキー情報を使って逆変換部により復号するように構成されている。暗号化に使用する受信信号は随時変化していくので秘話性の高い暗号化伝送システムを実現することができる。

【図面の簡単な説明】

【図1】従来の暗号化伝送システムの一例を示すブロック図。

【図2】この発明による暗号化伝送システムの一実施例を示すブロック図。

【図3】図2の動作例を説明するための各信号の変化を示す表。

【図4】この発明の伝送システムにおける暗号化通信装置の一実施例を示すブロック図。

【図5】暗号化通信装置の他の実施例を示すブロック図。

【図6】ランダムパタン生成回路の一実施例を示すブロック図。

【図7】図6における非線形演算回路の実施例を示すブロック図。

【図8】ランダムパタン生成回路の他の実施例を示すブロック図。

【図9】ランダムパタン生成回路の他の実施例を示すブロック図。

【図10】暗号化通信装置の更に他の実施例を示すブロック図。

【図11】図10におけるパタン縮退回路の実施例を示すブロック図。

【図12】図10のパタン縮退回路の入出力関係を示す表。

【図13】暗号化通信装置の更に他の実施例を示すブロック図。

【図14】暗号化通信装置の更に他の実施例を示すブロック図。

【図15】暗号化伝送システムの他の実施例を示すブロック図。

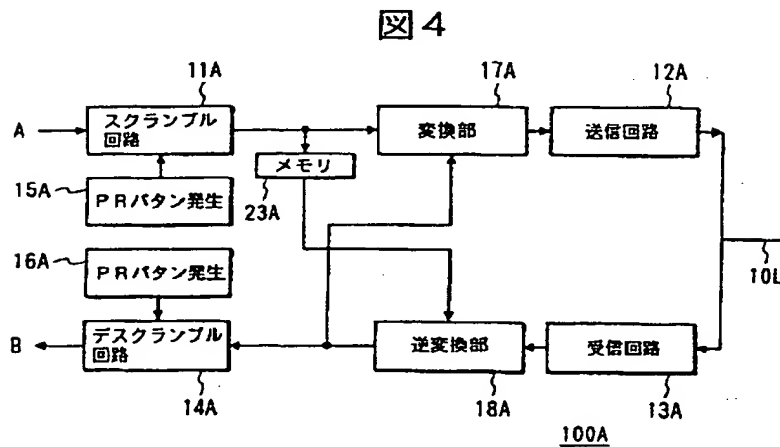
【図16】暗号化伝送システムの更に他の実施例を示すブロック図。

【図17】この発明の暗号化伝送システムにおける同期形時分割多重による交信例を示すタイムチャート。

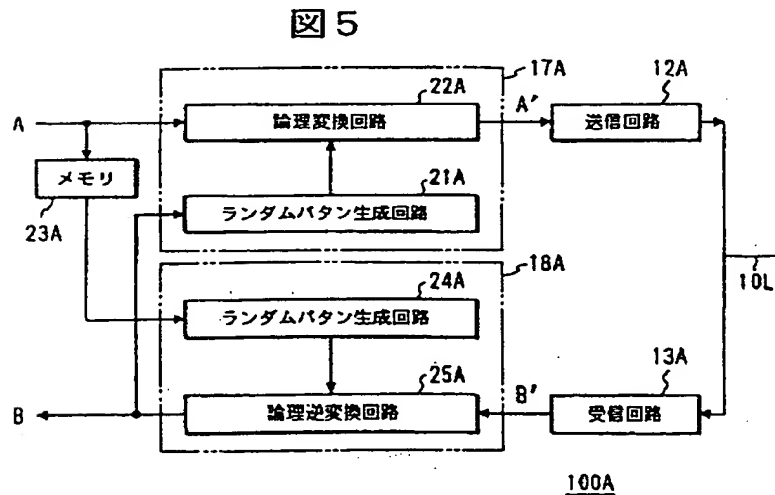
【図18】この発明の暗号化伝送システムにおける非同期形時分割多重による交信例を示すタイムチャート。

【図19】上り信号と下り信号に別々の伝送線路を設けたこの発明の暗号化伝送システムにおける交信例を示すタイムチャート。

【図4】

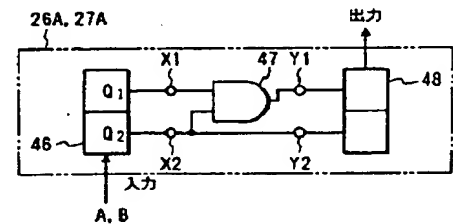


【図5】



【図11】

図11



【図12】

図12

表Ⅱ

入力		出力	
X1	X2	Y1	Y2
0	0	0	0
0	1	0	1
1	0	0	0
1	1	1	1

【図1】

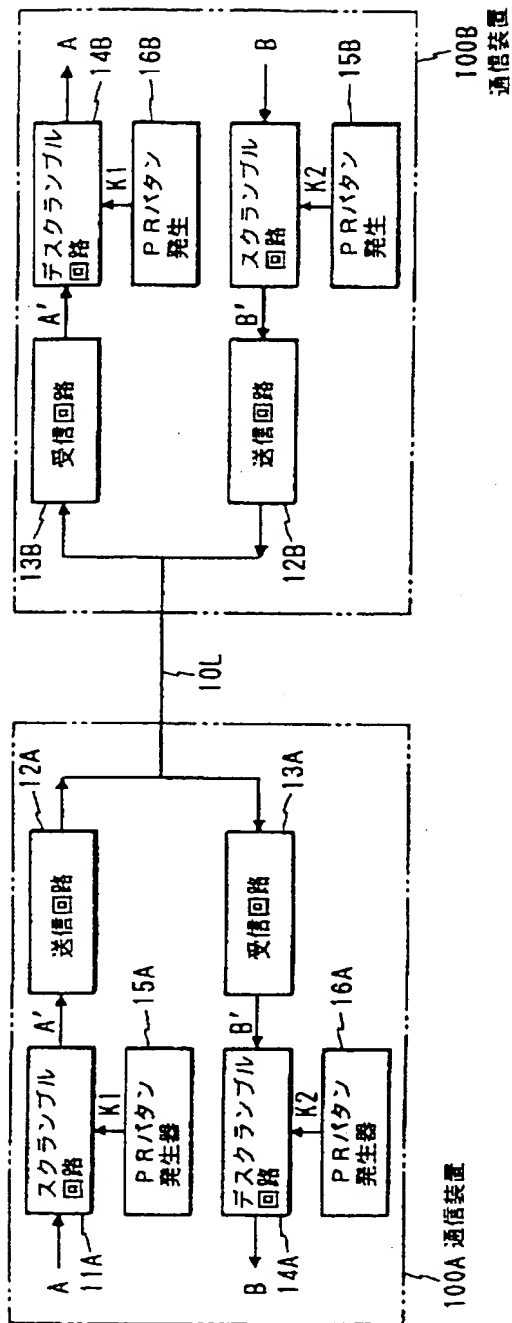


図 1

【図2】

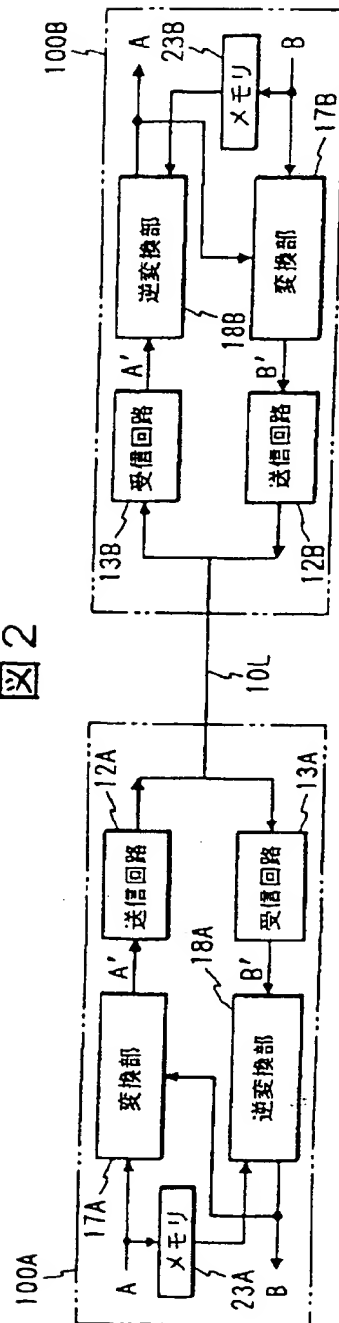
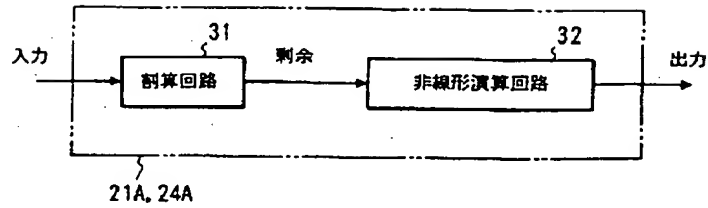


図 2

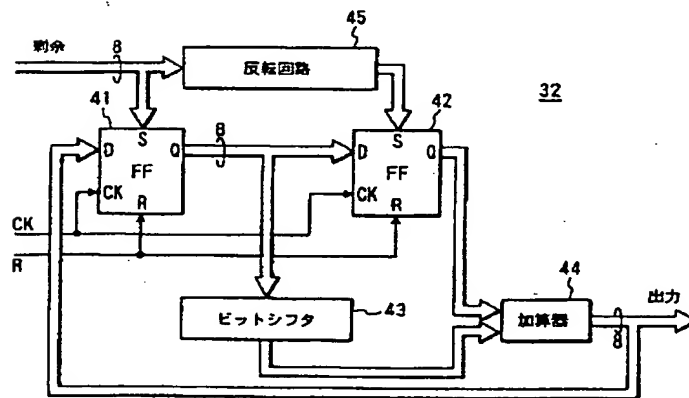
【図6】

図6



【図7】

図7



【図8】

図8

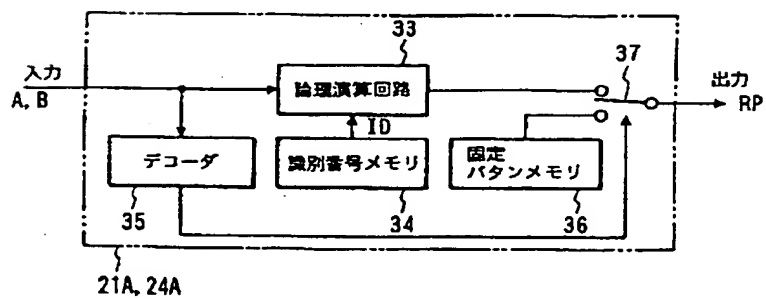


图 9

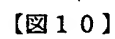


图 10

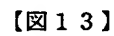
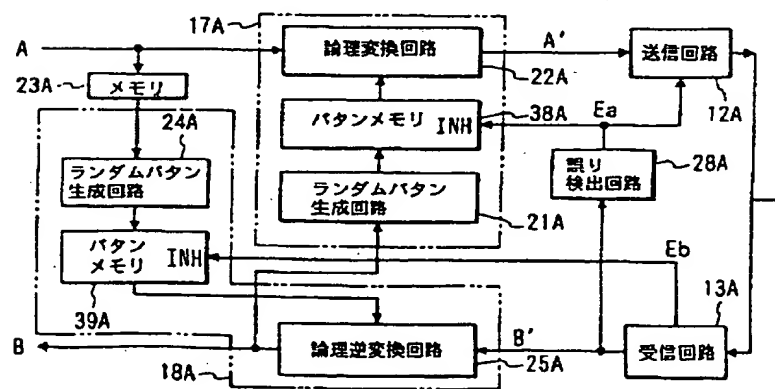
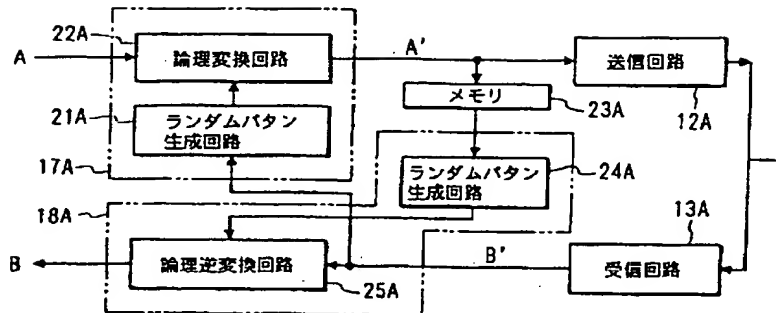


图 13



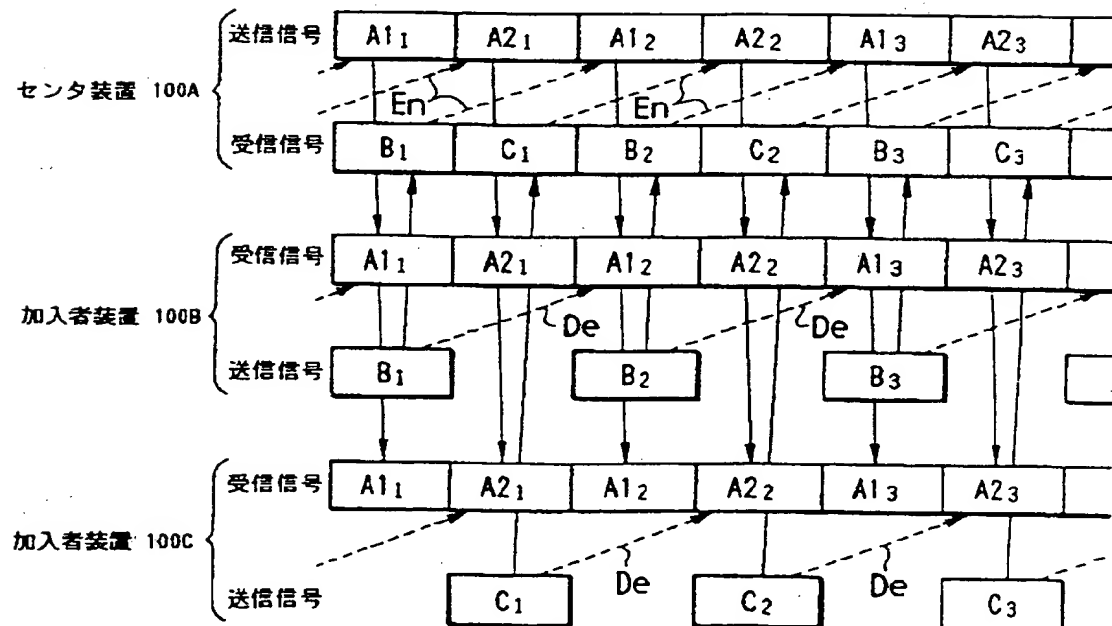
【図14】

図14



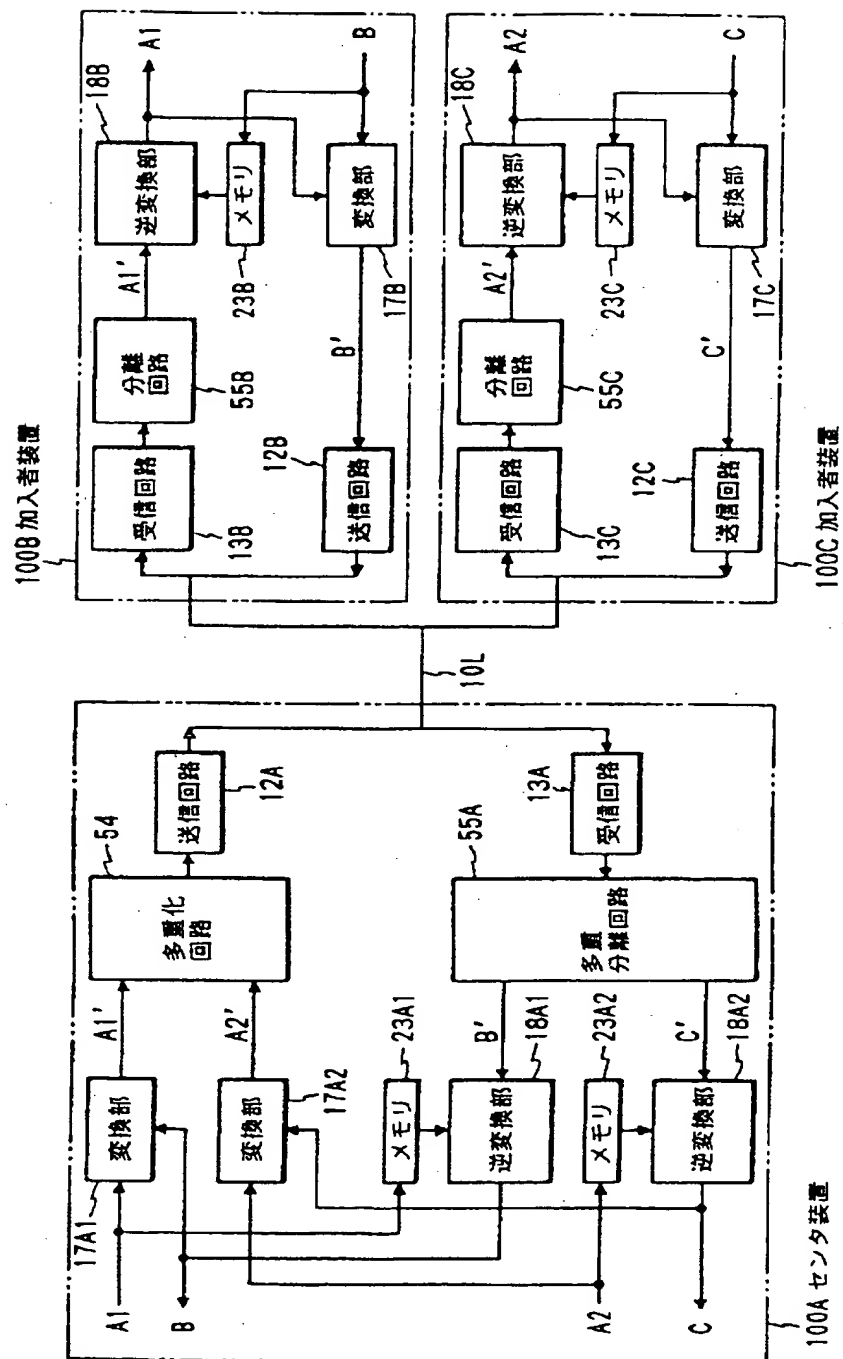
【図19】

図19

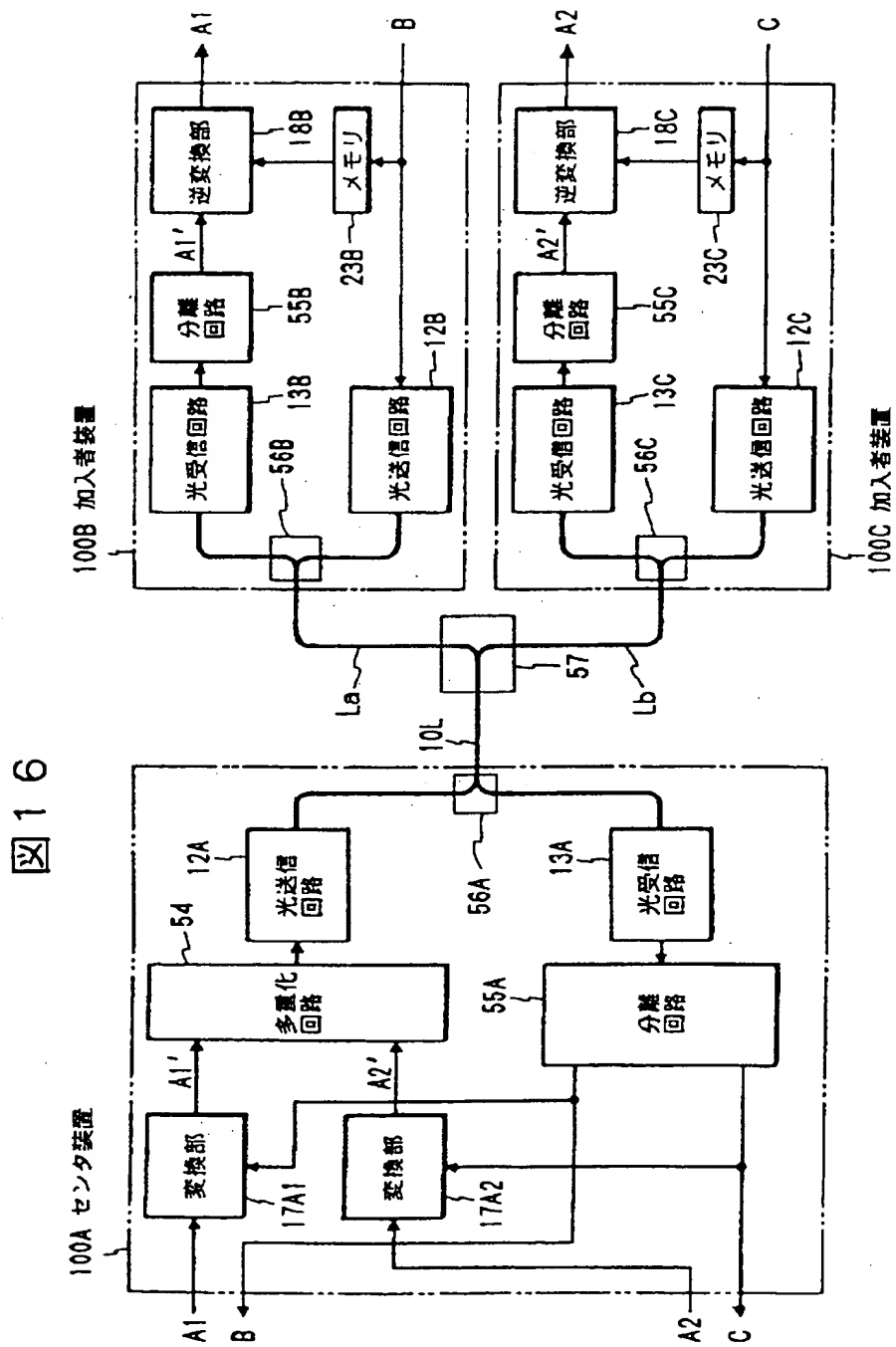


【図15】

図15

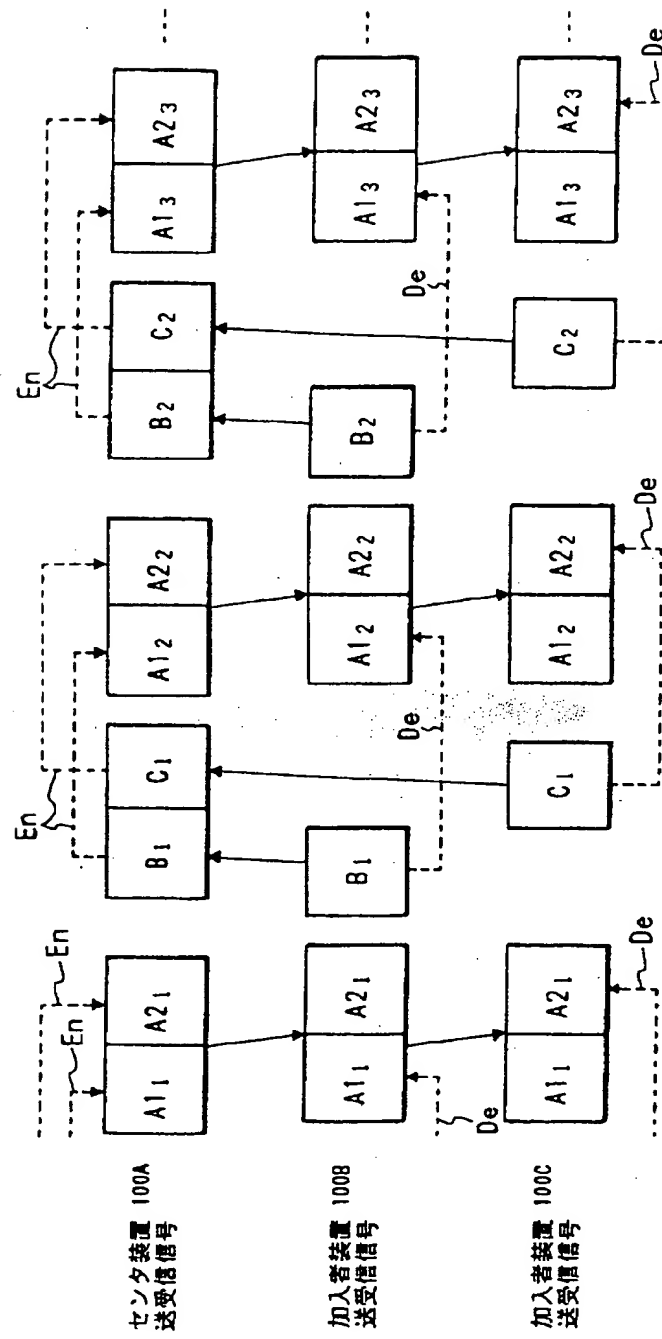


【図16】



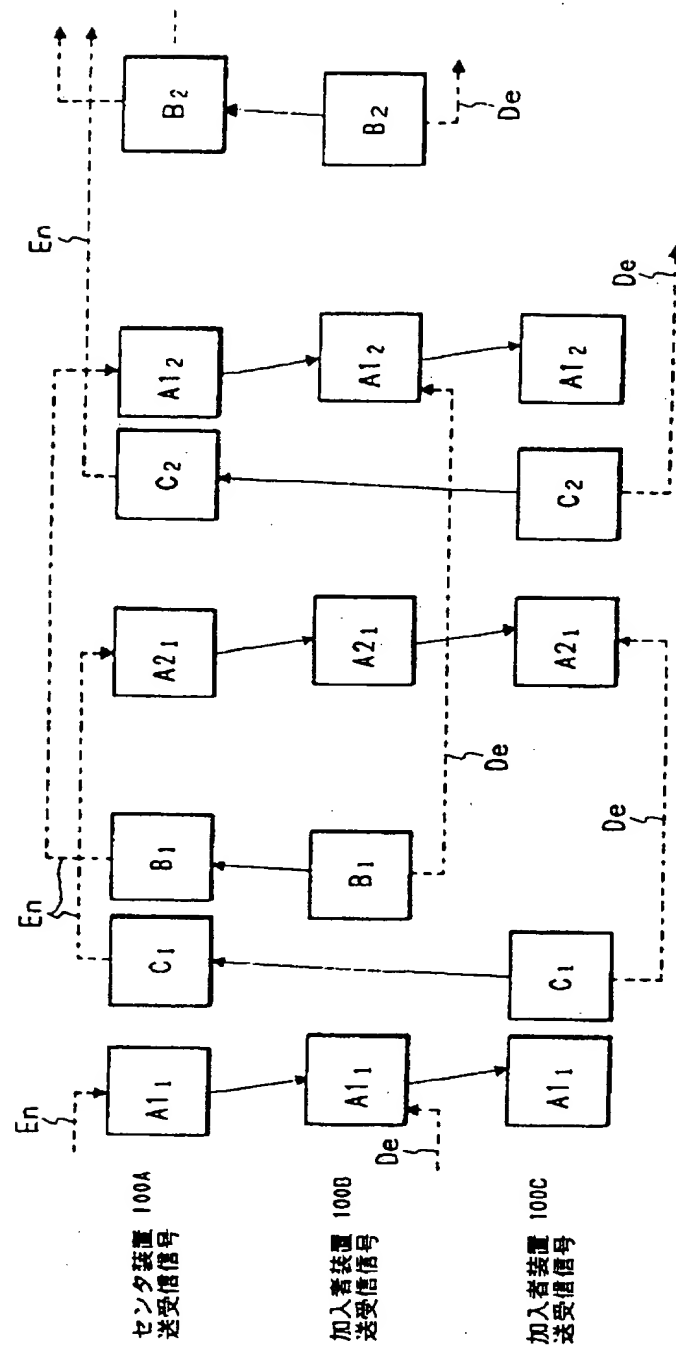
【図17】

図17



【図18】

図18



フロントページの続き

(72) 発明者 雲崎 清美
 東京都千代田区内幸町1丁目1番6号 日
 本電信電話株式会社内

(72) 発明者 三鬼 準基
 東京都千代田区内幸町1丁目1番6号 日
 本電信電話株式会社内